



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
[www.uspto.gov](http://www.uspto.gov)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/544,172	08/02/2005	Audrius Berzanskis	008-03US1	1533
53590	7590	10/28/2008	EXAMINER	
OPTICUS IP LAW, PLLC 7791 ALISTER MACKENZIE DRIVE SARASOTA, FL 34240				PATEL, NIRAV B
ART UNIT		PAPER NUMBER		
2435				
MAIL DATE		DELIVERY MODE		
10/28/2008		PAPER		

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

<b>Office Action Summary</b>	<b>Application No.</b>	<b>Applicant(s)</b>	
	10/544,172	BERZANSKIS ET AL.	
	<b>Examiner</b>	<b>Art Unit</b>	
	NIRAV PATEL	2435	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

#### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

- 1) Responsive to communication(s) filed on 02 August 2005.  
 2a) This action is FINAL.                    2b) This action is non-final.  
 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

- 4) Claim(s) 1-5 is/are pending in the application.  
 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.  
 5) Claim(s) \_\_\_\_\_ is/are allowed.  
 6) Claim(s) 1-5 is/are rejected.  
 7) Claim(s) \_\_\_\_\_ is/are objected to.  
 8) Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

- 9) The specification is objected to by the Examiner.  
 10) The drawing(s) filed on 02 August 2005 is/are: a) accepted or b) objected to by the Examiner.  
     Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
     Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).  
 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).  
 a) All    b) Some \* c) None of:  
     1. Certified copies of the priority documents have been received.  
     2. Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.  
     3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)            | 4) <input type="checkbox"/> Interview Summary (PTO-413)           |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)   | Paper No(s)/Mail Date. _____ .                                    |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date <u>11/08/05</u> .  | 6) <input type="checkbox"/> Other: _____ .                        |

## DETAILED ACTION

1. This action is in response to the application filed on Aug. 02, 2005.
2. Claims 1-5 are under examination.

### Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

3. Claims 1-5 are rejected under 35 U.S.C. 103(a) as being unpatentable over Thomas Jennewein et al. ("Quantum Cryptography with Entangled Photons", 1999) and in view of Muratani et al (US Patent. No. 7,194,090).

As per claim 1, Thomas Jennewein discloses a method for establishing a secure key between two stations[Fig. 2], the method comprising: exchanging single photons signals between two quantum key distribution stations to form a plurality of raw keys at each station [Fig. 2, page 4729 left col. lines 8-11, right col. lines 1-2]; performing error correction and privacy amplification on the raw keys to form a plurality of privacy amplified keys at each station [page 4729 right col. lines 1-7, page 4731 right col. lines 23-26]; wherein the at least one expanded key is suitable for one-time pad encryption of

information to be exchanged between the two stations [Fig. 3, page 4729 left col. lines 15-17].

Muratani teaches buffering the keys in each station to form matching key schedules at each station; and forming at least one expanded key from key selected from the matching key schedules [Fig. 10, 11, 16, 17 associated texts].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Muratani with Thomas Jennewein, since one would have been motivated to avoid or reduce a delay time in generating an expanded key [Muratani, col. 3 lines 16-18].

As per claim 2, the rejection of claim 1 is incorporated and Thomas Jennewein teaches:  
a) encrypting information using the at least one expanded key as a one-time pad; and b)  
transmitting the encrypted information between the two stations [Fig. 2, 3].

As per claim 3, Thomas Jennewein discloses a method of sending encrypted information between two stations [Fig. 2], the method comprising: establishing a raw key between the two stations using quantum key distribution [Fig. 2, page 4729 left col. lines 8-11, right col. lines 1-2]; establishing a privacy amplified key from the establish raw key [page 4729 right col. lines 1-7, page 4731 right col. lines 23-26]; sending encrypted information between the two station using a one-time pad based on either the unexpanding key or the expanded key [Fig. 3, page 4729 left col. lines 15-17].

Muratani teaches providing the encrypting data using a one-time pad based on an expanded version of the privacy amplified key as an expanded key [Fig. 10, 11, 16, 17 associated texts].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Muratani with Thomas Jennewein, since one would have been motivated to avoid or reduce a delay time in generating an expanded key [Muratani, col. 3 lines 16-18].

As per claim 4, the rejection of claim 3 is incorporated and Muratani teaches:

a) expanding one or more of the privacy amplified keys; and b) storing at each station the one or more expanded keys in a key schedule [Fig. 10, 11, 16, 17 associated texts].

As per claim 5, the rejection of claim 3 is incorporated and Muratani teaches:

a) storing at each station one or more unexpanded keys in a first key schedule; b) storing at each station one or more expanded keys in a second key schedule; and c) encrypting information using one-time pads based on keys from at least one of the first and second key schedules when raw keys cannot be exchanged between the stations [Fig. 10, 11, 16, 17 associated texts].

### **Conclusion**

4. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Nishioka et al (US Pub. No. 2005/0157875) -- Cryptographic communication apparatus

Alexios Beveratos et al (Single photon quantum cryptography, 2002)

Norbert Lutkenhaus (Security against individual attacks for realistic quantum key distribution, 2000)

Any inquiry concerning this communication or earlier communications from the examiner should be directed to NIRAV PATEL whose telephone number is (571)272-5936. The examiner can normally be reached on 8 am - 4:30 pm (M-F).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a

Application/Control Number: 10/544,172  
Art Unit: 2435

Page 6

USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

*/N. P./  
Examiner, Art Unit 2435  
/Kimyen Vu/*

*Supervisory Patent Examiner, Art Unit 2431*